the Senior Agency Official. Such authority has been delegated to Deputy Assistant Secretaries, Principal Officers at consulates general and consulates abroad, and certain other officers within the Department and at posts abroad. In the absence of the Secret or Confidential classification authority, the person designated to act for that official may exercise that authority.

§ 9.6 Derivative classification.

(a) *Definition.* Derivative classification is: the incorporating, paraphrasing, restating, or generating in new form information that is already classified and the marking of the new material consistent with the classification of the source material, or the marking of the information in accordance with an authorized classification guide. Duplication or reproduction of existing classified information is not derivative classification. Persons who apply classification markings derived from source material or as directed by a classification guide need not possess original classification authority.

(b) *Responsibility.* Information classified derivatively from other classified information shall be classified and marked in accordance with instructions from an authorized classifier or in accordance with an authorized classification guide and shall comply with the standards set forth in sections 2.1–2.2 of the Executive Order and 32 CFR 2001.22. The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years except for:

(1) Information that would reveal the identity of a confidential human source or a human intelligence source (50X1–HUM) or key design concepts of weapons of mass destruction (50X2–WMD), and

(2) Specific information incorporated into the classification guide under section 2.2(e) of the Executive Order relating to exemptions from automatic declassification.

(c) *Department of State Classification Guide.* The Department of State Classification Guide (DSCG) is the primary authority for the classification of information in documents created by Department of State personnel. The Guide is classified ''Confidential'' and is found on the Department of State's classified Web site.

§ 9.7 Identification and marking.

(a) Classified information shall be marked pursuant to the standards set forth in section 1.6 of the Executive Order, 32 CFR part 2001, subpart C, and internal Department guidance in 5 Foreign Affairs Manual.

(b) Foreign government information shall retain its original classification markings or be marked and classified at a U.S. classification level that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(c) Information assigned a level of classification under predecessor executive orders shall be considered as classified at that level of classification despite the omission of other required markings.

(d) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

§ 9.8 Classification challenges.

(a) *Challenges.* Authorized holders of information pertaining to the Department of State who believe that its classification status is improper are expected and encouraged to challenge the classification status of the information. Such persons making challenges to the classification status of information shall not be subject to retribution for such action. Informal, usually oral, challenges are encouraged. Formal challenges to classification actions shall be in writing to an original classification authority (OCA) with jurisdiction over the information and a copy of the challenge shall be sent to the Office of Information Programs and Services (IPS) of the Department of State, SA–2, 515 22nd St. NW., Washington, DC 20522–8100. The Department (either the

OCA or IPS) shall provide an initial response in writing within 60 calendar days.

(b) *Appeal procedures and time limits.* A negative response may be appealed to the Department's Appeals Review Panel (ARP) and should be sent to: Chairman, Appeals Review Panel, c/o Director, Office of Information Programs and Services/Appeals Officer, at the IPS address given above. The appeal shall include a copy of the original challenge, the response, and any additional information the appellant believes would assist the ARP in reaching its decision. The ARP shall respond within 90 calendar days of receipt of the appeal. A negative decision by the ARP may be appealed to the Interagency Security Classification Appeals Panel (ISCAP) referenced in section 5.3 of Executive Order 13526. If the Department fails to respond to a formal challenge within 120 calendar days or if the ARP fails to respond to an appeal within 90 calendar days, the challenge may be sent directly to the ISCAP.

(c) *Pre-publication review materials.* The provisions for classification challenges do not apply to material required to be submitted for pre-publication review, or other administrative action, pursuant to a non-disclosure agreement.

§9.9 Declassification and downgrading.

(a) *Declassification processes.* Declassification of classified information may occur:

(1) After review of material in response to a Freedom of Information Act (FOIA) request, mandatory declassification review request, discovery request, subpoena, classification challenge, or other information access or declassification request;

(2) After review as part of the Department's systematic declassification review program;

(3) As a result of the elapse of the time or the occurrence of the event specified at the time of classification;

(4) By operation of the automatic declassification provisions of section 3.3 of the Executive Order with respect to material more than 25 years old.

(b) *Downgrading.* When material classified at the Top Secret level is reviewed for declassification and it is determined that classification continues to be warranted, a determination shall be made whether downgrading to a lower level of classification is appropriate. If downgrading is determined to be warranted, the classification level of the material shall be changed to the appropriate lower level.

(c) *Authority to downgrade and declassify.* (1) Classified information may be downgraded or declassified by:

(i) The official who originally classified the information if that official is still serving in the same position and has original classification authority;

(ii) A successor in that capacity if that individual has original classification authority;

(iii) A supervisory official of either if the supervisory official has original classification authority;

(iv) Other Department officials specifically delegated declassification authority in writing by the Secretary or the Senior Agency Official; or

(v) The Director of the Information Security Oversight Office pursuant to Sec. 3.1(a) of E.O. 13526.

(2) The Department shall maintain a record of Department officials specifically designated as declassification and downgrading authorities.

(d) *Declassification in the public interest.* Although information that continues to meet the classification criteria of the Executive Order or a predecessor order normally requires continued protection, in some exceptional cases the need to protect information may be outweighed by the public interest in disclosure of the information. When such a question arises, it shall be referred to the Secretary or the Senior Agency Official for decision on whether, as an exercise of discretion, the information should be declassified and disclosed. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural right subject to judicial review.

(e) *Public disclosure of declassified information.* Declassification of information is not, by itself, authorization for its public disclosure. Previously classified information that is declassified may be exempt from public disclosure under the FOIA, the Privacy Act, or